AP-51XX v2.3.4.0-008R – Release Notes

Introduction
New Features
AP-51XX Hardware/ Software Compatibility Matrix
AP-51XX Default Configurations
Firmware Update
Resetting the AP-51XX Password
AP-51XX MAC Addresses
Known Issues & Recommendations
Fixes

Introduction – AP-5131 Indoor AP & AP-5181 Outdoor AP

Designed to address the wireless and wired connectivity needs of the small office or retail outlet, the AP-5131 provides a single-box solution which integrates all services required to extend secure broadband access to mobile users. With the ability to connect local users to a remote private network via a secured IPSec link, the AP-5131 is ideal for deployment in branch offices or at telecommuter sites for enterprise-class WLAN performance and secure connectivity of wired clients. The AP-5131 integrates a Router and DHCP Server for local LAN connectivity; a configurable stateful inspection firewall for LAN isolation; a VPN endpoint for secure backhaul connectivity; a QoS Engine for superior performance of real time video and voice applications; and a AAA server with Hotspot Gateway for security and public access management. With v1.1 or newer, the AP-5131 offers a self-assembling, self-healing Mesh Networking architecture designed to extend the reach of the wireless network via wireless communication between Access Points.

This Maintenance Release is based on 2.3.0.0. V2.3.4.0 includes fixes for certain defects that have been reported by customers and/or found internally.

Customers are only entitled to convert to this release of the software if they have a valid Motorola service agreement or are covered under warranty. Customers who currently have a support contract in place will be able to download the software from a protected Web site (this requires registering and requesting the software, as well as verifying the service contract). Customers who do not have a support agreement will be provided options to purchase a Motorola service contract.

New Features in version 2.3.4.0-008R

Apache web server in AP is upgraded in this release.

Following new features are included in this Release. These features are available only from CLI.

1. **EAP throttling**

   Ability to limit the number of wireless clients doing simultaneous 802.1x EAP authentications.

```
admin(network.wireless)>set max-eap-connections <5-100>
```

```
admin(network.wireless)>set radio-eap-throttle mode <enable/disable>
admin(network.wireless)>set radio-eap-throttle clear-threshold <1-100>
admin(network.wireless)>set radio-eap-throttle timeout <1-3600>
```

Default values are max-eap-connections – 10, radio-eap-throttle mode disabled, radio-eap-throttle clear-threshold 5, and radio-eap-throttle timeout 5 seconds.

2. **Configurable broadcast multicast transmit speed**

Ability to send broadcast traffic on highest or lowest basic rate.

```
admin(network.wireless.radio.802-11bg)>set bcmc-tx-speed ?

  <op-mode>                       : op-mode - (range, throughput)
```

When range is selected the lowest of basic rate would be used for all broadcast/multicast transmissions. When throughput is selected, the highest of basic rate would be used for all broadcast/multicast transmissions. Default setting is 'range'.

3. **Proxy ARP for wireless clients**

Ability of an AP to proxy ARP for wireless clients to reduce number of broadcast traffic on air. Default is dynamic.

```
admin(network.wireless)>set proxy-arp ?

  <op-mode><cr>                   : op-mode - (strict, dynamic, disable)
```

4. **Opportunistic PMK caching**

Ability of AP to cache last 3 PMKids for wireless client.

OPMK uses WNMP multicast messages to sync MU's PMK among AP's on the same subnet. The supplicant should be capable of doing OPMK. The AP will keep up to 3 PMK's for each associated MU. The AP will reuse the oldest slot for the MU when it runs out of slots. The lifetime for each key will be 1 hour. Total number of key cache will be 1250. The AP will flush the entire key cache if it gets full. The AP will force the MU to do 802.1x authentication if it does not find the MU in the key cache. The AP will delete the MU's PMK if it fails WPA handshake.The AP independently expires entries in its key cache. It does not tell other APs to remove them.

```
admin(network.wireless.security.edit)>set ccmp opp-pmk-caching ?

  <mode><cr>                      : mode - (enable,disable)
```

5. **Configurable Differentiated Service Code Point (DSCP) qos mapping**

Support for DSCP QoS mapping in the radio configuration.

```
admin(network.wireless.radio)>set qos-mapping(wired-to-wireless) dscp ?
```

```
<dscp-num><tid-num><cr>          : 0-63 Specify the DSCP value(0-63) to be
con.
                                 : tid-num:
                                 : tid0: best effort category traffic
                                 : tid1: background category traffic
                                 : tid2: background category traffic
                                 : tid3: best effort category traffic
                                 : tid4: video traffic category traffic
                                 : tid5: video traffic category traffic
                                 : tid6: voice traffic category traffic
                        : tid7: voice traffic category traffic
```

6. **Configurable roam notification timing**

   Ability to configure when to send roam notification after mobile client association. Options will be after MU has associated and after MU state becomes data ready. Default setting - after MU association.

```
admin(network.wireless.wlan)>set roam-notification <after-assoc, after-
data-ready>
```

7. **AP reset on ethernet inactivity**

   Option to reset AP if there is inactivity on LAN interface. To enable AP reset, configure LAN ethernet timeout and reset-interval. Default setting is - no reset.

```
admin(network.lan)>set ?
  reset-interval                 : set reset interval on ethernet
connection timeout

admin(network.lan)>set reset-interval ?
  <period><cr>                   : period - 0 (no reset)
                                 : period 1-1000 min.
```

8. **802.11 authentication request throttling**

   Ability to limit the number of wireless clients doing simultaneous 802.11 authentications.

```
admin(network.wireless)>set max-auth-mus <1 – 127>
admin(network.wireless)>set radio-auth-throttle mode <enable/disable>
admin(network.wireless)>set radio-auth-throttle clear-threshold <1 – 127>
admin(network.wireless)>set radio-auth-throttle timeout <1 – 3600> in 100ms
```

   Defaults will be mode disabled, max-auth-mus – 50, clear-threshold 30, timeout – 10 (in 100 ms) equals 1 second.

AP-51XX Hardware/ Software Compatibility Matrix

	v1.0.0.0 v1.0.1.0 v1.1.0.0	v1.1.1.0	v1.1.2.0	v2.0.0.0-045R	v2.1.0.0-030R	**v2.3.4.0-008R**

AP-5131	Supported	Supported	Supported	Supported	Supported	Supported
AP-5181	Not-Supported	Supported	Supported	Supported	Supported	Supported
AP-5131 & AP-5181 with new processor revision (July 2007)	Not-Supported	Not-Supported	Supported	Supported	Supported	Supported
AP-5131 Dependent Mode AP-5131-40020-D-WR AP-5131-13040-D-WR	Not-Supported	Not-Supported	Not-Supported	Supported	Not - Supported	Not - Supported

AP-51XX Default Configurations

	v1.0.0.0 v1.0.1.0	v1.1.0.0	v1.1.1.0 v1.1.2.0 v2.0.0.0-045R v2.1.0.0-030R V2.1.1.0-001R V2.2.0.0-023R V2.2.1.0-007R V2.2.2.0-001R V2.3.0.0 V2.3.1.0 V2.3.2.0 V2.3.3.0 V2.3.4.0
WAN	DHCP client Auto-update enabled	Static IP: 10.1.1.1 Static Mask: 255.0.0.0	Static IP: 10.1.1.1 Static Mask: 255.0.0.0
LAN1 (a.k.a LAN)	Static IP: 192.168.0.1 Static Mask: 255.255.255.0 DHCP Server enabled	DHCP Client Auto-update enabled Default Gateway* Ethernet Port Enabled	DHCP Client Auto-update enabled Default Gateway* Ethernet Port Enabled
LAN2	n/a	Static IP: 192.168.1.1 Static Mask: 255.255.255.0 DHCP Server Enabled	Disabled
Access via WAN Port	HTTPS, SSH, SNMP: enabled	HTTP, HTTPS, Telnet, SSH, SNMP: enabled	HTTP, HTTPS, Telnet, SSH, SNMP: enabled

*DNS and Domain Name parameters take effect on the Default Gateway Interface.

Firmware Update

Note: Upgrading from 1.0 to 2.X is a two step process which requires the same upgrade procedure to be repeated twice. The first upgrade will result in a bootloader change and the second upgrade will result in a firmware change. For subsequent upgrades a single download will suffice. Using Auto Update, the AP will automatically update itself twice when upgrading to v2.X

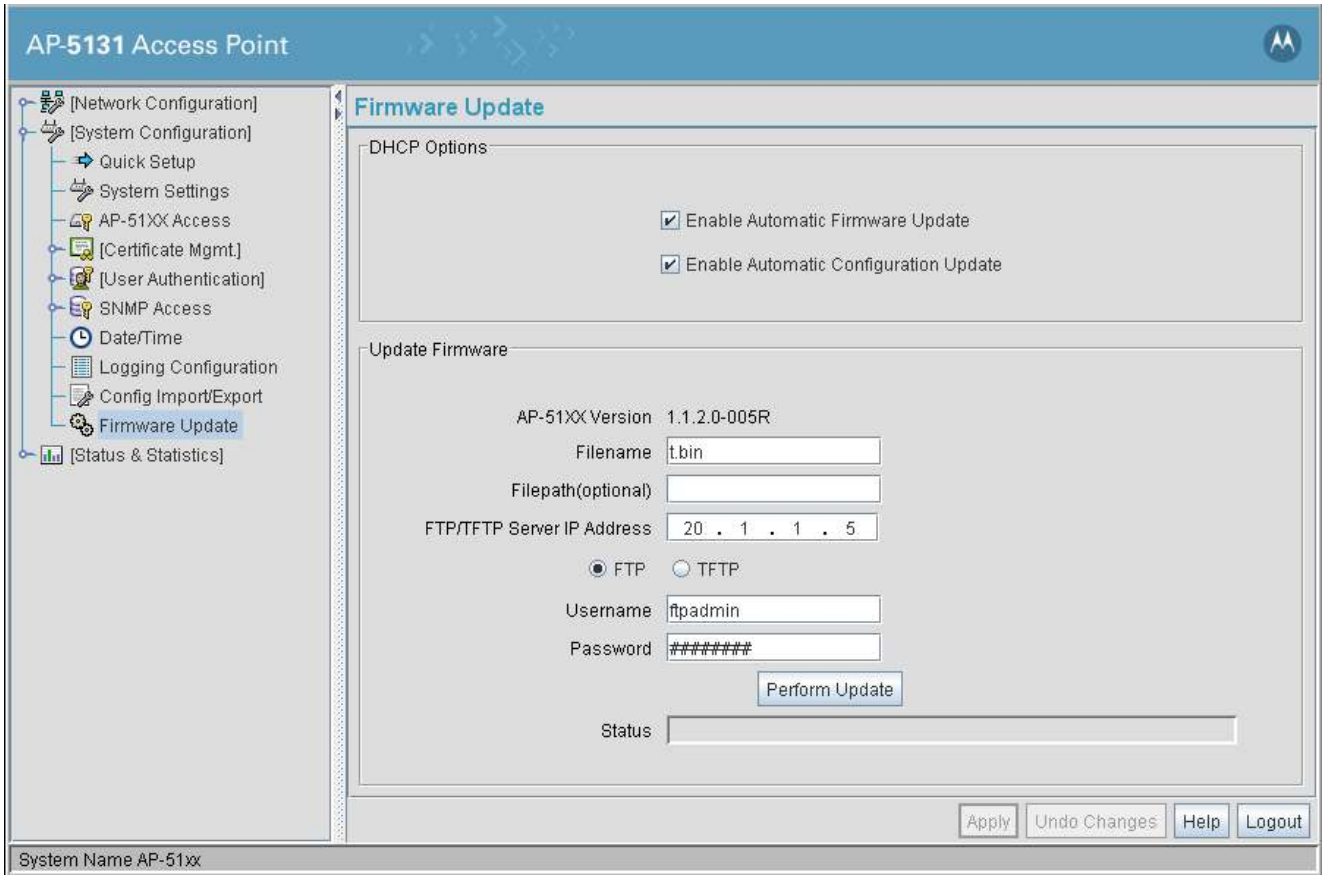
Note: Upgrading from 1.0/1.1/1.1.1/1.1.2 to 2.X retains the existing settings. It is recommended, however, that users export their 1.0/1.1/1.1.1/1.1.2 configuration for backup purposes prior to upgrading.

Note: When downgrading from v1.1.2 to v1.0, all configuration settings are lost and the AP will return to factory defaults.

Note: Dependent Mode AP-5131's (with a D in the Part Number) cannot be downgraded to any software version below 2.0.0.0-045R.

To conduct a firmware update on the AP-51XX from 1.X to 2.X:

1. Select 'System Configuration' → 'Firmware Update' from the AP-51XX menu tree of the GUI.
2. Specify the name of the target firmware file within the 'Filename' field.
3. If the target firmware file resides within a directory, specify a complete path for the file within the 'Filepath (optional)' field.
4. Enter an IP address for the FTP or TFTP server used for the update.
5. Use the drop-down menu to specify the FTP or TFTP server's location. Select the appropriate button, FTP or TFTP, for the server's location. The server can reside on the WAN or on the LAN.
6. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
7. Set the following FTP parameters if applicable:
    - Username - Specify a username for the FTP server login.
    - Password - Specify a password for FTP server login.



8. Click 'Apply'.
9. Click the 'Perform Update' button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update. This step may take several minutes.

10. After the AP reboots, return to the 'Firmware Update' screen.
11. Repeat Step #9.
12. After the AP reboots, clear the browser cache and return to the 'Firmware Update' screen. Check the Status field to verify whether the firmware update was successful.

Resetting the AP-51XX Password

The AP-51XX *Command Line Interface* (CLI) enables users who forget their password to reset it to the factory default. Only an installation professional should reset the access point's password and promptly define a new restrictive password.
To contact Motorola Support in the event of a password reset requirement, go to www.symbol.com/contactsupport.

AP-51XX MAC Addresses

The AP-51XX has one MAC address for each LAN, which are displayed in 'LAN Stats' and 'WAN Stats', under the 'Status and Statistics' page in the Web User Interface.

Each radio on an AP-51XX supports four Basic Service Sets (BSS). Each BSS, has a corresponding MAC address. The MAC address, which is displayed in the Web Interface, under the Radio Settings screen, corresponds to that of BSS #1. The MAC addresses for the other three BSS's (BSS #2, #3, #4) are derived by adding 1, 2, 3, respectively, to the radio MAC address (same as BSS #1).

For example: If the radio MAC address displayed under the Radio Settings screen (Network Configuration → Wireless → Radio Configuration → Radio<n>) is 00:23:68:72:20:DC, then the BSSs for that radio will have the following MAC addresses:

BSSID	MAC Address	Hexadecimal Addition
BSSID#1	00:23:68:72:20:DC	Same as Radio MAC Address
BSSID#2	00:23:68:72:20:DD	Radio MAC Address + 1
BSSID#3	00:23:68:72:20:DE	Radio MAC Address + 2
BSSID#4	00:23:68:72:20:DF	Radio MAC Address + 3

Known Issues & Recommendations

Recommendation: AP-51x1 access points participating in a mesh topology should use the same firmware version.

Known Issues:

1. Wireless client disassociation after configuration change. (CQ: 10751): After applying certain changes to the configuration, wireless clients may temporarily become disconnected as each radio resets.
2. Mesh Network Connectivity while making changes to a Base or Client Bridge node: Mesh connectivity may temporarily be unavailable when making configuration changes to Base or Client Bridge APs.
3. If using the Radius time-based authentication feature to authenticate access point user permissions, ensure UTC has been selected from the Date and Time Settings screen's Time Zone field. If UTC is not selected, time based authentication will not work properly.
4. Rogue AP Detection Command (CQ: 29889): The "Add all to allowed list" command in the Rogue AP Detection screen may result in the Active Allowed AP List not being updated correctly.

5. VPN Configuration Import (CQ: 29576): The AP-51XX will not import a VPN configuration if the tunnel name parameter contains a space in the text.
6. AP-4131 vs. AP-51XX Default Basic Rates Setting: The default Basic Rates setting for the AP-51XX is 1, 2, 5.5 and 11 Mbps. The AP- 4131's default Basic Rates setting was 1 & 2 Mbps only. Note that this difference may cause interoperability problems with certain older wireless devices. The default setting can be changed in the AP-51XX
7. Java GUI does not load in web browser: If the Java Web User Interface does not load in the browser it may be that a previous version of the html page is being stored in the browser's cache. To solve this problem, clear the browser cache and set the browser to always download web pages.
8. When downgrading a unit from 2.2 to 2.1.1 it is important to rename WLANs and remove special characters from WLANs as these were not supported in 2.1.1.
9. CLI (CQ52436): CLI 'show routes' will not immediately display routes correctly after a route is added/deleted. Workaround is to wait 1 minute between. adding/deleting routes before using 'show routes' command.
10. DHCP Lease Information (CQ53499): Legacy Symbol Netvision phone devices will not be listed in the DHCP Lease information.
11. Static routes will only be shown if destination is reachable (CQ52083).
12. Current set of invalid characters across GUI and CLI -> space < > | " & , \ ?
13. CPU utilization might spike incorrectly when AP is handling a lot of traffic.
14. If WAN port is not connected – static routes will not be shown.
15. Upgrading to 2.3.2.0 and above from previous releases will add source port as "ALL" by default in IPfilter rules.
16. CLI displays sftp option for cfg import/export and fw update but is not supported in AP5131(CQ68189). No impact on any functionality
17. AP5131 getting crashed if booting process interrupted using "ctrl+c" (CQ67626)
18. SIP packets are dropped by AP5131 with SIP server across VPN (CQ67321)
19. After every reboot/upgrade, getting unnecessary messages in console (CQ66993). No end user impact for this
20. WSP need to be able to get "Avg MU noise" from AP even if there are no MUs associated (CQ62309)
21. "PTK Bad replay ctr" with message #1 seen in syslog with MUs on WPA/TKIP security (CQ60346). No end user impact
22. GUI shows error while mapping WLAN to user group (CQ 91144). CLI can be used to configure the same.

Fixes

Version v2.3.4-008R includes several enhancements/fixes:

SPR/CQ Ref ID	Description
21705	Sporadic AP Crashes
21715	The access ports AP5131 v 2.3.3.1 are not reporting to the ADSP appliance as sensors.
21911	Intermittently cannot downgrade the AP5131 from 2.3.3.1-003R back to 2.3.2.0-0008R.
21916	AP5131 with 2.3.3 and cc Oman doesn't allow to use 5GHz radio. It should be permitted accoring to regulatory.

22698	AP5131 Apache version 1.3.41 under firmware v2.3.3.0-06R Version not PCI compliant
22830	LAN 1 port configured for 100mb/FD connected to Nortel Bayswitch (100mb/FD), goes to 100mb/HD, after reboot.
TRION00058768	The default value for Native VLAN tag for LAN Ports is set to 'tagged'. By Industry standard it should be Untagged.
TRION00083199	When SFTP is used for configuration export, the status shows “Done” even though it fails.
TRION00085179	Firmware upgrade fails when one radio is configured as sensor and discovered in ADSP
TRION00085182	SFTP support for configuration import/export and firmware upgrade.
TRION00086463	Base Bridge crashes in wireless mesh setup
TRION00086506	Sensor does not come online in ADSP when AP is connected over WAN interface unless LAN IP is configured and enabled.
TRION00100593	MU Inactivity Timer issue